What is claimed is:

1.   .   A method of providing secure access to a service on a service web server comprising:

        (a)   maintaining at a permission web server a first permission, wherein the first permission comprises a label related to the service and a digital signature of a first user;

        (b)   providing access to the first permission to a second user upon said second user authenticating to said permission web server;

        (c)   providing the second user a permission comprising the first permission and a permission link comprising the label and a digital signature of the permission web server;

        (d)   receiving at the service web server from said second user a request to access the service;

        (e)   receiving the permission from the second user at the service web server;

        (f)   verifying the digital signature of the permission web server and the digital signature of the first user in the permission; and

        (g)   providing the second user access to the service if step (f) produces a positive result.

2.   The method of claim 1 wherein the first and second user are the same.

3.   The method of claim 1 wherein the label comprises a URL for identifying the service.

4.   A system for providing secure access to a service on a service web server comprising:

       · a permission web server that maintains a first permission, wherein the first permission comprises a label related to the service and a digital signature of a first user; that provides a second user access to the first permission upon the second user authenticating to the permission web server; and that provides the second user a permission comprising the first permission and a permission link comprising the label and a digital signature of the permission web server; and

the service web server that receives from the second user a request to access the service and the permission; that verifies the digital signature of the permission web server and the digital signature of the first user in the permission; and that provides the second user access to the service if the verification produces a positive result.

5.   A method of providing secure access to a service on a service web server comprising:

(a)   maintaining at a permission web server a first permission, wherein the first permission comprises a label related to the service and a digital signature of a first user;

(b)   providing access to the first permission to a second user upon said second user authenticating to said permission web server;

(c)   providing the second user a permission comprising the first permission and a permission link comprising the label and a digital signature of the permission web server;

(d)   receiving at the service web server from a subsequent user a request to access the service, the subsequent user having been delegated a subsequent permission comprising the permission;

(e)   receiving the subsequent permission from the subsequent user at the service web server;

(f)   verifying at least the digital signature of the permission web server and the digital signature of the first user in the permission; and

(g)   providing the subsequent user access to the service if step (f) produces a positive result.

6.   The method of claim 5 wherein the subsequent permission is delegated to the subsequent user via electronic mail.

7.   The method of claim 5 wherein the subsequent permission is delegated to the subsequent user by a subsequent web server.

8.   A system for providing secure access to a service on a service web server comprising:

a permission web server that maintains a first permission, wherein the first permission comprises a label related to the service and a digital signature of a first user; that provides a second user access to the first permission upon the second user authenticating to the permission web server; and that provides to the second user a permission comprising the first permission and a permission link comprising the label and a digital signature of the permission web server; and

the service web server that receives from a subsequent user a request to access the service and a subsequent permission, comprising the permission, the subsequent user having been delegated the subsequent permission; that verifies at least the digital signature of the permission web server and the digital signature of the first user in the permission; and that provides the subsequent user access to the service if the verification produces a positive result.